

IN THE CLAIMS

Claims 1-40 are pending.

Claims 1, 18 and 31 are currently amended.

Claims 1, 18 and 31 are independent.

1. (Currently amended) A method comprising:

sequentially storing pointers to a plurality of results provided by a stream cipher output rule in a first, second, and third storage units;
providing a plurality of results from a pairing function, the pairing function pairing individual values from the first and third storage units that are at least a threshold value apart wherein the pairing function is $p(x, y) = x \oplus (ay + b)$, where a and b are two constants, and a is odd or $p(x, y) = \gamma, \delta$ is chosen as a nearly universal hash function by the iteration of the following rules:

$$\underline{\alpha = ax \bmod 2^{2n}}$$

$$\underline{\beta = by \bmod 2^{2n}}$$

$$\underline{\gamma = \alpha^L + \beta^R \bmod 2^{2n}}$$

$$\underline{\delta = \alpha^R + \beta^L \bmod 2^{2n}}$$

where x^L and x^R respectively denote the left and right halves of x , and a, b are chosen randomly; and

upon reaching the threshold value of the output rule results, serially and recursively rotating contents of the first, second, and third storage units, wherein the contents of the storage units are the pointers.

2. (Original) A method as recited by claim 1, wherein a short-term correlation between the individual values from the first and third storage units are limited.

3. (Original) A method as recited by claim 1, wherein a length of each of the first, second, and third storage units equals the threshold value.

4. (Original) A method as recited by claim 1, wherein the first, second, and third storage units are implemented in a single memory device.

5. (Original) A method as recited by claim 1, wherein the serial rotation is performed by shifting the first, second, and third storage units in a same direction.

6. (Original) A method as recited by claim 1, wherein the pairing function results are stored in a table.

7. (Original) A method as recited by claim 1, wherein the method is utilized to strengthen an output of a stream cipher keystream generator.

8. (Original) A method as recited by claim 1, wherein only the first and third storage units are active at any given time.

9. (Original) A method as recited by claim 1, wherein the first and third storage units are initialized with random values.

10. (Original) A method as recited by claim 1, wherein the method is applied recursively.

11. (Original) A method as recited by claim 1, wherein the output rule is combined with one or more update rules selected from a group comprising random walks, T-functions, LFSRs (linear feedback shift registers), and word-based stream ciphers.

12. (Original) A method as recited by claim 11, wherein the random walks are selected from one or more walks in a group comprising an additive walk, a multiplicative walk, a Gabber-Galil walk, a Ramanujan walk, a permutation walk, and a random walk with a dynamic generator.

13. (Original) A method as recited by claim 1, further comprising enhancing the pairing function by utilizing a fourth storage unit.

14. (Original) A method as recited by claim 13, wherein the fourth storage unit is walked through using a one-cycle secret permutation.

15. (Original) A method as recited by claim 14, wherein the secret permutation slowly mutates.

16. (Original) A method as recited by claim 13, wherein the fourth storage unit is initialized with random values.

17. (Original) A method as recited by claim 13, wherein the fourth storage unit is initialized with random values and a variable delay.

18. (Currently amended) A system comprising:

a processor;

a system memory coupled to the processor;

sequentially storing pointers to a plurality of results provided by a stream cipher output rule in a first, second, and third portion of the system memory;

providing a plurality of results from a pairing function, the pairing function pairing individual values from the first and third portions of the system memory that are at least a threshold value apart wherein the pairing function is $p(x, y) = x \oplus (ay + b)$, where a and b are two constants, and a is odd or $p(x, y) = \gamma, \delta$ is chosen as a nearly universal hash function by the iteration of the following rules:

$$\underline{\alpha = ax \bmod 2^{2n}}$$

$$\underline{\beta = by \bmod 2^{2n}}$$

$$\underline{\gamma = \alpha^L + \beta^R \bmod 2^{2n}}$$

$$\underline{\delta = \alpha^R + \beta^L \bmod 2^{2n}}$$

where x^L and x^R respectively denote the left and right halves of x , and a, b are chosen randomly; and

upon reaching the threshold value of the output rule results, serially and recursively rotating contents of the first, second, and third portions of the system memory, wherein the contents of the system memory are the pointers.

19. (Original) A system as recited by claim 18, wherein a short-term correlation between the individual values from the first and third portions of the system memory are limited.

20. (Original) A system as recited by claim 18, wherein a length of each of the first, second, and third portions of the system memory equals the threshold value.

21. (Original) A system as recited by claim 18, wherein the first, second, and third portions are implemented in multiple memory devices.

22. (Original) A system as recited by claim 18, wherein the serial rotation is performed by shifting the first, second, and third portions in a same direction.

23. (Original) A system as recited by claim 18, wherein the pairing function results are stored in a table on the system memory.

24. (Original) A system as recited by claim 18, wherein the system is utilized to strengthen an output of a stream cipher keystream generator.

25. (Original) A system as recited by claim 18, wherein the first and third portions are initialized with random values.

26. (Original) A system as recited by claim 18, wherein the output rule is combined with one or more update rules selected from a group comprising random walks, T-functions, LFSRs (linear feedback shift registers), and word-based stream ciphers.

27. (Original) A system as recited by claim 26, wherein the random walks are selected from one or more walks in a group comprising an additive walk, a multiplicative walk, a Gabber-Galil walk, a Ramanujan walk, a permutation walk, and a random walk with a dynamic generator.

28. (Original) A system as recited by claim 18, wherein an operation of the pairing function is enhanced by utilizing a fourth portion of the system memory.

29. (Original) A system as recited by claim 28, wherein the fourth portion is initialized with random values.

30. (Original) A system as recited by claim 28, wherein the fourth portion is initialized with random values and a variable delay.

31. (Currently amended) One or more computer-readable media having instructions stored thereon that, when executed, direct a machine to perform acts comprising:

strengthening an existing stream cipher's output by sequentially storing pointers to a plurality of results provided by the stream cipher in a first, second, and third storage units;

providing a plurality of results from a pairing function, the pairing function pairing individual values from the first and third storage units that are at least a threshold value apart, wherein the pairing function is $p(x, y) = x \oplus (ay + b)$, where a and b are two constants, and a is odd or $p(x, y) = \gamma, \delta$ is chosen as a nearly universal hash function by the iteration of the following rules:

$$\underline{\alpha = ax \bmod 2^{2n}}$$

$$\underline{\beta = by \bmod 2^{2n}}$$

$$\underline{\gamma = \alpha^L + \beta^R \bmod 2^{2n}}$$

$$\underline{\delta = \alpha^R + \beta^L \bmod 2^{2n}}$$

where x^L and x^R respectively denote left and right halves of x , and a, b are chosen randomly;

upon reaching the threshold value of the existing stream cipher output, serially and recursively rotating contents of the first, second, and third storage units, thereby strengthening the cipher stream, wherein the contents of the storage units are the pointers; and
outputting the now strengthened stream cipher.

32. (Previously presented) One or more computer-readable media as recited by claim 31, wherein a short-term correlation between the individual values from the first and third storage units is limited.

33. (Original) One or more computer-readable media as recited by claim 31, wherein a length of each of the first, second, and third storage units equals the threshold value.

34. (Original) One or more computer-readable media as recited by claim 31, wherein the first, second, and third storage units are implemented in a single memory device.

35. (Original) One or more computer-readable media as recited by claim 31, wherein the serial rotation is performed by shifting the first, second, and third storage units in a same direction.

36. (Original) One or more computer-readable media as recited by claim 31, wherein the pairing function results are stored in a table.

37. (Original) One or more computer-readable media as recited by claim 31, wherein the acts are performed recursively.

38. (Previously presented) One or more computer-readable media as recited by claim 31, wherein the existing stream cipher is combined with one or more update rules selected from a group comprising random walks, T-functions, LFSRs (linear feedback shift registers), and word-based stream ciphers.

39. (Original) One or more computer-readable media as recited by claim 38, wherein the random walks are selected from one or more walks in a group comprising an additive walk, a multiplicative walk, a Gabber-Galil walk, a Ramanujan walk, a permutation walk, and a random walk with a dynamic generator.

40. (Original) One or more computer-readable media as recited by claim 31, further comprising enhancing the pairing function by utilizing a fourth storage unit.